Technical Information

Recorders, Data Loggers, and Control Products Security Standard

TI 04A02A01-00EN

Contents

1. Introduction 1-1

Why Security Is Essential 1-1

Applicable Products 1-2

Trademarks 1-2

2. Assets That Should Be Protected 1-3

3. Identifying and Evaluating Threats 1-4

Identifying and Evaluating Vulnerabilities 1-4

Risk Assessment 1-5

4. Overview of the Products That This Document Applies To 1-6

Communication Protocols 1-6

5. Security Threats 1-11

6. Product-Specific Security Features 1-12

GX10/GX20/GP10/GP20 Paperless Recorders and GM Data Acquisition System . 1-12

MW100 Data Acquisition Units 1-12

DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000 Paperless Recorders .. 1-13

CX1000/CX2000 Paperless Recorders 1-13

DX100P/DX200P Paperless Recorders 1-14

UTAdvanced Digital Indicating Controllers/Program Controllers/Digital Indicator with Alarms .. 1-14

YS1000 Series Single-loop Controllers 1-14

7. Staff Security 1-15

Revision Information i

The contents of this document are subject to change without notice.

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

TI 04A02A01-00EN

©Copyright June 2012

3rd Edition August 2015

1. Introduction

Information Security in Yokogawa Electric Corporation and its group companies

Yokogawa is committed to company-wide security measures, to protect information assets as an important business asset against threats such as leakage and destruction, to fulfill its social responsibility as a company that is trusted by customers and suppliers.

In order to protect information assets from threats, Yokogawa has established management rules to comply with the management regulations.

In the management rules, it is clearly stated responsible-management system and responsible person.

In the management rules, they are stated that how to respond to appropriate management and accident handling confidential information, equipment information, access rights, and software.

All officers and all employees company-wide in Yokogawa Group are required to comply with these.

In order to ensure compliance with the provisions of these regulations, we have to conduct internal audits and regular education.

Antivirus to information devices and storage media used in the security section, are set forth in the administrative rules.

In the management rules anti-virus is stated that it should be performed appropriately.

It also stated that portable media should be properly managed; the handling and management of access rights management.

Virus protections for products and distributions have been established both development and manufacturing phase in each business divisions, and performed by the standards.

This document contains security guidelines for products that Yokogawa's Network Solutions Business Division provides. This document provides generalized risk assessment and security measures for the network (Ethernet) connections of applicable products and uses standard models as a basis for explaining how to manage applicable products.

Because new measures are always being taken to counter today's ever-changing security threats, the contents of this document are subject to change without prior notice.

Why Security Is Essential

In recent years, with the advancement of network and information technology, open information technologies used in operating systems and communication protocols are also being adopted in control systems. This trend is accelerating the close interaction between information systems and control systems.

In this type of environment, control systems can become targets for attackers and are subject to security threats from computer viruses and other malicious programs. Ensuring the safety of measuring systems and control systems is vital to protecting important assets.

Applicable Products

This document applies to the following products.

- Chart recorders μR10000/μR20000
- Paperless recorders GX10/GX20/GP10/GP20, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX100P/DX200P, CX1000/CX2000
- Data acquisition system GM
- Data acquisition units MW100
- Single-loop controllers YS1000 Series
- Digital indicating controllers/
  Program controllers/
  Digital indicator with alarms UTAdvanced

Trademarks

- Ethernet is a registered trademark of Fuji Xerox Corporation.
- Modbus is a registered trademark of Schneider Automation Inc. in the United States.
- Other company and product names are registered trademarks or trademarks of their respective holders.
- In this document, the TM and ® symbols do not accompany their respective registered trademark or trademark names.

2. Assets That Should Be Protected

You need to make a list of assets that should be protected, clarify their owners, and evaluate their values. The higher the value of the asset, the greater the need to take security measures. The following are examples of assets that should be protected.

Data Assets

- Production schedule information
- System configuration information
- Application configuration information
- Control parameter information
- Recipe information
- History information

Device Assets

- Engineering workstations (EWSs)
- Operator consoles (OITs)
- Process controllers (DCSs and PLCs)
- Field devices
- Network devices

Human and Environmental Assets

- Employees
- Factories and plant facilities
- Natural environment

When theses assets are exposed to security threats, the following may result:

- Disturbance or halting of production activities
- Leakage of recipes and other confidential information that relates to production activities
- Personal injury
- Damage to factories and plant facilities
- Environmental damage

These events can inflict tremendous losses on an organization.

The objective of taking security measures is to protect these assets from threats and reduce opportunity losses incurred by the organization.

Priority Classification Example

Below is an example of how asset priorities can be classified.

- Priority A: Extremely high
- Priority B: High
- Priority C: Low
- Priority D: Extremely low

NOTE

This document is based on “ISA 99.00.01-2007: Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models.” This document refers to this standard as ISA 99.00.01.

ISA 99.00.01 defines “activity-based criteria” for determining security measures and “asset-based criteria” for determining the assets that need to be protected. This document is based on these criteria.

3. Identifying and Evaluating Threats

Determine all possible security threats to the assets that are on your list of assets that need to be protected. Possible threats need to be considered from the following viewpoints.

Unauthorized Access to Assets by Individuals with Malicious Intent

- Insider
- Outsider
- Via network
- Direct access to assets (direct operation of instruments that contain assets)

Unauthorized Access to Assets by Malicious Software

- Via network
- Via removable media

Inappropriate Access by Valid Users through Operation Errors and Careless, Unintended Acts

- Via network
- Via removable media
- Direct access to assets (direct operation of instruments that contain assets)

For each security threat that you have identified, evaluate the probability of occurrence. Below is an example of how the probabilities of occurrence can be classified.

- Probability level A: High probability that the threat will occur
- Probability level B: Moderate probability that the threat will occur
- Probability level C: Low probability that the threat will occur

Identifying and Evaluating Vulnerabilities

Determine the vulnerability of each asset or the vulnerability of the device that contains the asset. Vulnerabilities are conditions that allow security threats to adversely affect assets. Examples of vulnerabilities are listed below.

- Flaws in the planning of security measures
- Flaws in the execution of security measures
- Flaws in the supervision or improvement of security measures
- Lack of physical protection
- Flaws in the configuration of firewalls
- Failure to exterminate viruses and flaws in the application of security patches
- Flaws in backing up data (system is not being backed up)
- Insufficient understanding of production control systems and their operation and environment
- Lack of system designer and operator awareness about security

Risk Assessment

Assess the security risk for each asset or the device containing the asset. Risk is assumed to be expressible using the following formula.

Risk = threat × vulnerability × expected loss

Risk assessment enables you to prioritize various security measures. Risk assessment includes assessing the business loss incurred due to the halting of system functionality, the expenses required to repair the damage to the production control system, and so on.

Determine the priority of each security measure in accordance with the level of quantitative loss. Doing so will enable you to determine which risks require countermeasures, which risks can be tolerated, and so on.

Note that in some cases, losses are difficult to assess as business losses because they include factors such as environmental contamination, personal injury, and loss of public confidence in the organization.

4. Overview of the Products That This Document Applies To

Applicable Products

This document applies to the following products.

- Chart recorders μR10000/μR20000
- Paperless recorders GX10/GX20/GP10/GP20, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX100P/DX200P, CX1000/CX2000
- Data acquisition system GM
- Data acquisition units MW100
- Single-loop controllers YS1000 Series
- Digital indicating controllers/
  Program controllers/
  Digital indicator with alarms UTAdvanced

The communication features implemented on the applicable products vary depending on the product series. This chapter describes the communication features that are implemented on each series of products and the security measures that should be considered.

Features of Applicable Products

All the products covered in this document use microprocessors and real-time OSs to run communication applications. At the factory, different communication applications are embedded in each product series.

In principle, users cannot add new program codes to or create new applications in these instruments. As an exception, some products do allow users to update the embedded software. However, only specific code can be embedded in a specific way, so there is no threat of software updates leading to the introduction of malicious programs into these instruments.

Communication Protocols

Ethernet and TCP/IP Protocol

Applicable products come with standard or optional 10BASE-T or 100BASE-TX Ethernet ports. Ethernet communication uses stable TCP and UDP protocols that are based on IPv4.

The applicable products allow IP addresses, subnet masks, and default gateways to be specified.

In addition, on applicable products equipped with client features, destination devices can be specified by their IP address or by their DNS (Domain Name System) host name.

The port numbers in the following table are factory default port numbers that have been allotted for the purpose of connecting to the server features of the applicable products. The port numbers of some products are fixed. Fixed port numbers are indicated as “fixed” in the table.

Server Features of GX10/GX20/GP10/GP20 Paperless Recorders and GM Data Acquisition System

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	4	Modbus	Multi-vendor connection (Modbus server)
21/tcp	4	FTP	File transfer (FTP server)
80/tcp or 443/tcp (when Encryption is On)	-	HTTP or HTTPS (when Encryption is On)	www (HTTP server)
123/udp	-	SNTP	Time synchronization (SNTP server)
34434/tcp (fixed)	4	Yokogawa proprietary	General-purpose communication services

Server Features of MW100 Data Acquisition Units

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	4	Modbus	Multi-vendor connection (Modbus server)
21/tcp	4	FTP	File transfer (FTP server)
80/tcp	-	HTTP	www (HTTP server)
123/udp	-	SNTP	Time synchronization (SNTP server)
34318/tcp	4	Yokogawa proprietary	General-purpose communication services

Server Features of DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000 Paperless Recorders

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	2	Modbus	Multi-vendor connection (Modbus server) DX1000T/DX2000T/DX1000/DX2000 only
21/tcp	2	FTP	File transfer (FTP server)
80/tcp	-	HTTP	www (HTTP server)
123/udp	-	SNTP	Time synchronization (SNTP server)
34260/tcp (fixed)	3	Yokogawa proprietary	Setup and measurement services
34261/tcp (fixed)	1	Yokogawa proprietary	Maintenance and test services
34264/udp (fixed)	-	Yokogawa proprietary	Instrument information service

Server Features of DX100P/DX200P and CX1000/CX2000 Paperless Recorders

Port Number	Maximum Simultaneous Connections	Protocol	Service
21/tcp (fixed)	2	FTP	File transfer (FTP server)
80/tcp (fixed)	-	HTTP	www (HTTP server)
34260/tcp (fixed)	3	Yokogawa proprietary	Setup and measurement services
34261/tcp (fixed)	1	Yokogawa proprietary	Maintenance and test services
34264/udp (fixed)	-	Yokogawa proprietary	Instrument information service

Server Features of μR10000/μR20000 Chart Recorders

Port Number	Maximum Simultaneous Connections	Protocol	Service
34260/tcp (fixed)	3	Yokogawa proprietary	Setup and measurement services
34261/tcp (fixed)	1	Yokogawa proprietary	Maintenance and test services
34264/udp (fixed)	-	Yokogawa proprietary	Instrument information service

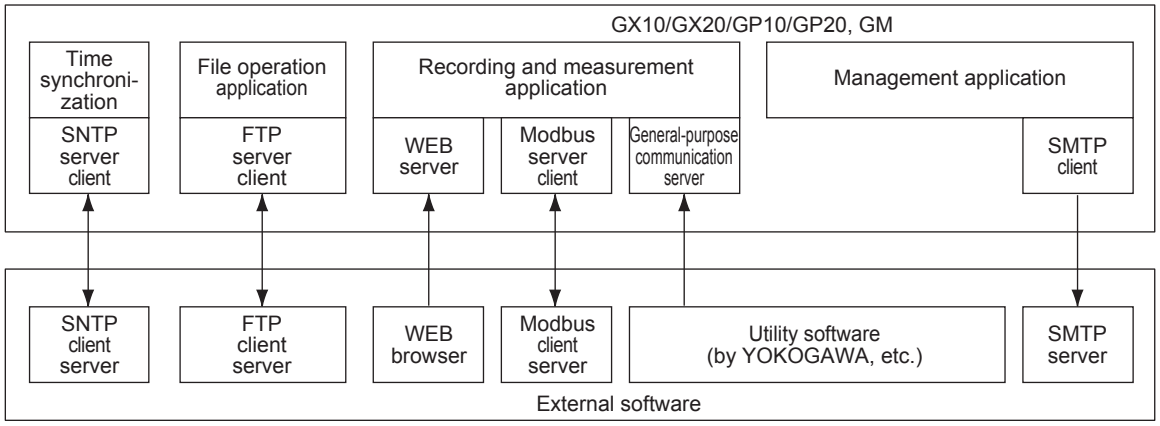
YS1000 Series Single-loop Controllers (Server features)

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	1	Modbus	Multi-vendor connection (Modbus server)

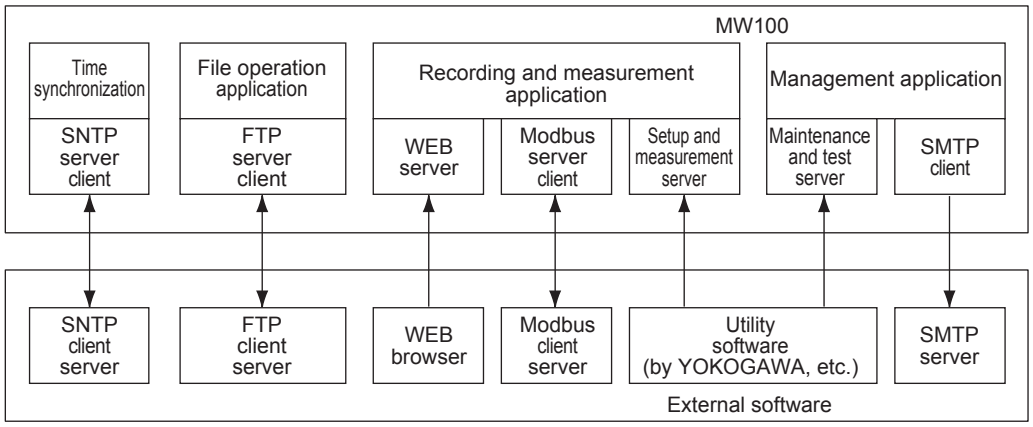
Server Feature of UTAdvanced Digital Indicating Controllers/Program Controllers/Digital Indicator with Alarms

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	2	Modbus	Multi-vendor connection (Modbus server)

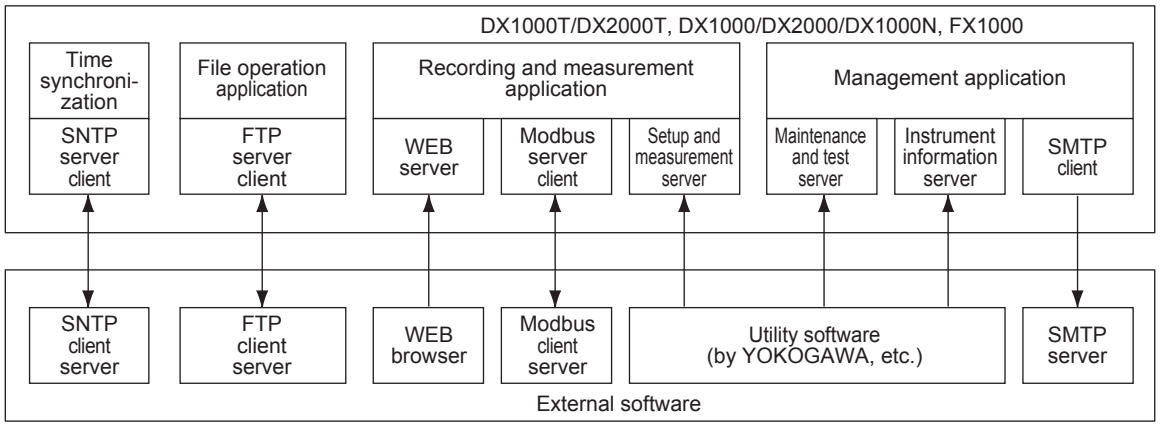
The following figure summarizes the client and server features of each instrument. An overview of each protocol is given in the later pages.



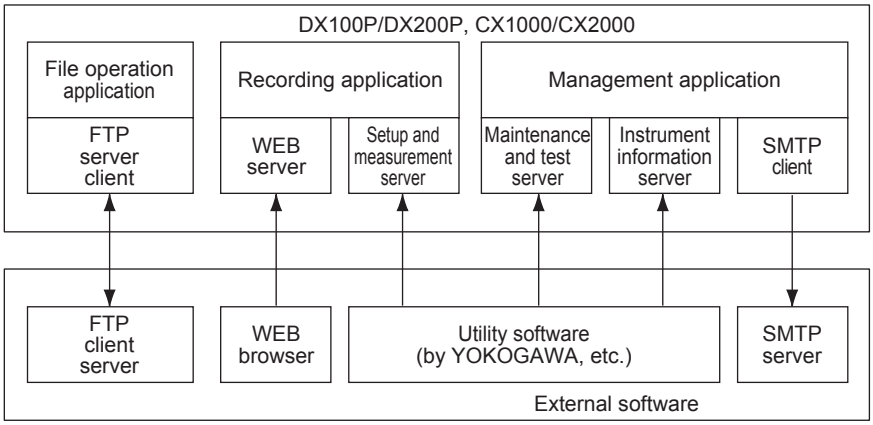
GX10/GX20/GP10/GP20 Paperless Recorders and GM Data Acquisition System



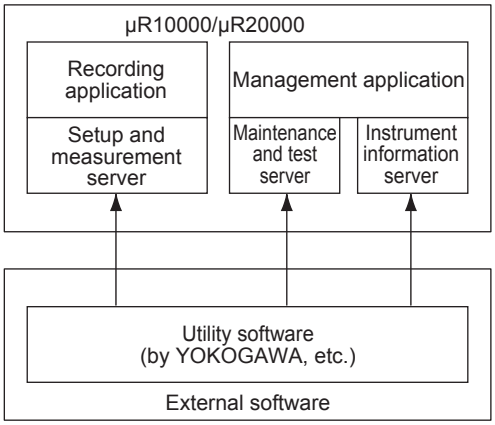
MW100 Data Acquisition Units



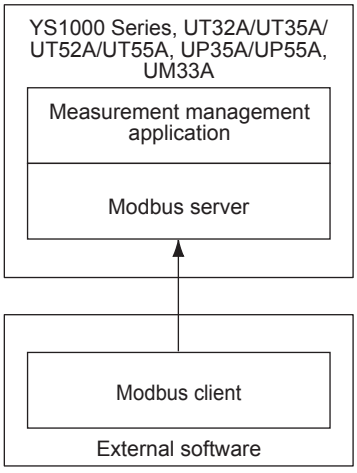
DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000 Paperless Recorders



DX100P/DX200P and CX1000/CX2000 Paperless Recorders



µR10000/µR20000 Chart Recorders



YS1000 Series Single-loop Controllers, UTAdvanced Digital Indicating Controllers/Program Controllers/ Digital Indicator with Alarms

FTP Protocol (Paperless recorders, data acquisition system and data acquisition units)

The file management application saves data residing in the main memory to files on an external storage medium. Depending on how the instrument is configured, the file management application generates daily, weekly, and other types of report files. These files are saved to an external storage medium (disk or memory card) that is inserted into the instrument.

The FTP server feature can be used to manipulate the files and directories in the external storage medium. The measurement and report files described above are stored in specified directories. Authenticated users can retrieve and delete existing files and save new files. If the FTP client feature is enabled, files can be automatically transferred to registered FTP servers when the files are created or when specific events occur. The FTP server has a user authentication feature. When the server's login feature (described later) is enabled, users can use the FTP server only when they enter the appropriate user name and password.

Up to two connection destination servers (primary and secondary) can be specified. For each, the user sets the server name (host name or IP address), user name, password, and initial directory. Under normal conditions, the instrument attempts to transfer files to the primary server. If the transfer fails, the instrument attempts to transfer files to the secondary server.

HTTP Protocol (Paperless recorders, data acquisition system and data acquisition units)

The recording application displays recording screens and messages on a remote Web browser. It also allows the instrument to be controlled remotely (only when the user logs in as an operator) via a Web browser. Microsoft Internet Explorer has been tested for operational compatibility. The HTTP server has a user authentication feature. When the server's login feature (described later) is enabled, users can use the HTTP server only when they enter the appropriate user name and password.

SMTP Protocol (Paperless recorders, data acquisition system and data acquisition units)

The management application transmits emails to an SMTP server in accordance with how the instrument has been set up. On the applicable products, emails are transmitted:

(1) Periodically

(2) When a hardware malfunction or other system error occurs

(3) When an hourly, daily, monthly, or other report is created

(4) When an alarm occurs due to measurement errors or other reasons

For each situation, you can set (1) whether to send an email, (2) the subject, (3) the destinations (whether to send email to each of two groups), (3) the body message, and (4) whether to include the Web address (URL) and measured values of each instrument.

Modbus protocol

(YS1000 Series, UTAdvanced, MW100, GM, GX10/GX20/GP10/GP20, DX1000T/DX2000T/DX1000/DX2000/DX1000N, and FX1000)

The Modbus protocol is widely used in communications between industrial devices. The protocol is also used to connect these devices to DCSs, PLCs, SCADAs, etc. For the GX10/GX20/GP10/GP20, GM, DX1000T/DX2000T, DX1000/DX2000/DX1000N, and FX1000, the Modus protocol can be used to output measured data and to start and stop measurements. For the YS1000 Series and UTAdvanced, the Modbus protocol can be used to change an instrument's settings, such as the SP, through the access and modification for the instrument's register values.

Yokogawa Proprietary Protocol

(Chart recorders, paperless recorders and data acquisition units)

The server feature in the recording application and management application uses a command-response protocol. This protocol makes it possible to read measured values, setup and measurement information, maintenance and test information, and instrument information. Commands and responses are primarily exchanged using ASCII character strings, but for some commands, binary response data is returned. The syntax and operations of commands and responses are defined in the user's manual of each instrument. The Yokogawa proprietary protocol has a user authentication feature. When the protocol's login feature (described later) is enabled, users can use the protocol only when they enter the appropriate user name and password.

5. Security Threats

Notable security threats are listed below.

Virus Infection Threats

There is no threat of the applicable instruments being infected with viruses. The operating system used in the instruments is a unique OS for embedded applications. In addition, off-the-shelf office applications, email clients, and browsers—which are often targets of viruses and macros—are not embedded in the instruments, so there is no worry about being compromised by viruses or macros through such programs. However, the DX, MW, and other instruments that use external storage may be used as storage (stepping stones) for files that contain viruses.

Intrusion Threats

The applicable instruments have multiple server features, and users can log into them. However, users cannot start other clients from the instruments, so the instruments cannot be used to intrude into other systems or to send obscure emails.

Network access to instruments' measured values and settings can be protected with passwords. To use a password to protect an instrument, enable the login feature in advance. Access to instruments is not possible unless the password is known. However, when you log into an FTP server, the user name and password are transmitted in plain text. If the network is wiretapped, it is possible for the password to be stolen.

There is always a possibility that a password may be leaked by a person who is not careful. There is a possibility of direct intrusion into the instruments when the instruments are installed at remote sites and connected via telephone lines. Damages that might occur are data leaks, destruction of settings, and damage to production facilities and products as a result of improper operation.

Threats of Information Leaks and Sabotage

Chart recorders, single-loop controllers, and digital indicating controllers hold very limited information about networks (IP addresses, subnet masks, default gateways, products' host and domain names, and DNS server addresses). Damages that may be incurred due to leaks of these pieces of information are equivalent to or less than damages that may be incurred due to leaks from personal computers.

On the other hand, paperless recorders and data acquisition units have FTP client and SMTP features. Therefore, these instruments have access information for external FTP servers and SMTP servers. Once a user is able to log into these instruments, it is possible for the user to obtain such information. If the access information is stolen as a result of a leak or eavesdropping of the login password, this may allow unauthorized intrusion into relevant servers.

If intrusion is allowed into instruments, measured values may be retrieved, settings may be destroyed, and output (control signals) may be operated inappropriately. For example, if a setting is changed externally and the controlled temperature is raised abnormally, produced goods may be damaged. Also, recorded data may be erased or tampered with.

6. Product-Specific Security Features

This chapter explains the security features of each system product. They should be assessed when security measures are put in place. Each product has features that enhance security.

GX10/GX20/GP10/GP20 Paperless Recorders and GM Data Acquisition System

Login Feature

The login feature allows only registered users to access the instruments. There are two user levels (privileges).

Administrator privileges:

All features can be used. Administrators can specify which features to make available to normal users.

Normal user privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Operation / setting authority can be set up individually.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the instruments and view measured data and who is able to access the instruments and change their measurement setups. Assign appropriate login privileges to users to ensure security. Up to 50 administrators and normal users can be registered in these instruments.

SSL Communication Function

Communication that sends and receives information encrypted by the SSL (Secure Socket Layer) protocol is possible. Public key encryption and certificate are used to encrypt communication and secure the connection. HTTP server and FTP server are supported.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

IP Access Limitation Function

Only Modbus access from a registered IP address is allowed. Access from an unregistered IP address is rejected. This feature prevents unauthorized access and enhances security.

MW100 Data Acquisition Units

Login Feature

The login feature allows only registered users to access the MW100. There are two user levels (privileges).

Administrator privileges:

All features can be used.

User privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Measurement range adjustments require administrator privileges.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the MW100 and view measured data and who is able to access the MW100 and change the measurement setup. Assign appropriate login privileges to users to ensure security. Up to 10 users can be registered in the MW100.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000 Paperless Recorders

Login Feature

The login feature allows only registered users to access the paperless recorders. There are two user levels (privileges).

Administrator privileges:

All features can be used. Administrators can specify which features to make available to normal users.

Normal user privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Measurement range adjustments require administrator privileges.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the paperless recorders and view measured data and who is able to access the paperless recorders and change their measurement setups. Assign appropriate login privileges to users to ensure security. Up to 5 administrators and 30 normal users can be registered in these paperless recorders.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

IP Access Limitation Function

(Available on the DX1000T/DX2000T/DX1000/DX2000/DX1000N Release 3 and later, restricts access to Modbus server)

Only Modbus access from a registered IP address is allowed. Access from an unregistered IP address is rejected. This feature prevents unauthorized access and enhances security.

CX1000/CX2000 Paperless Recorders

Login Feature

The login feature allows only registered users to access the paperless recorders. There are two user levels (privileges).

Administrator privileges:

All features can be used.

User privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Measurement range adjustments require administrator privileges.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the paperless recorders and view measured data and who is able to access the paperless recorders and change their measurement setups. Assign appropriate login privileges to users to ensure security. One administrator and up to six users can be registered in these paperless recorders.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

DX100P/DX200P Paperless Recorders

Login Feature

The login feature allows only registered users to access the paperless recorders. There are two user levels (privileges).

Administrator privileges:

All features can be used.

User privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Measurement range adjustments require administrator privileges.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the paperless recorders and view measured data and who is able to access the paperless recorders and change their measurement setups. Assign appropriate login privileges to users to ensure security. Up to 3 administrators and 90 users can be registered in these paperless recorders.

Audit Trail Feature

The audit trail feature saves operation logs, configuration change logs, and the setup files that were in use. Up to 2000 operation log entries can be recorded in the internal memory. You can review the operation log to verify what kinds of operations have been performed in the past.

Sign Record Feature

The sign record feature adds batch processing results (pass or fail), comments, the names of users who added information, and the date and time that the information was added to the display data and event data files that are stored to external storage media. The information is embedded in files along with tampering detection data and can thus be used as digital signatures.

Log Information

DX100P/DX200P operations, configuration changes, error messages, file transfers using the FTP client feature, email transmissions, Web interface operations, SNTP server access logs, etc., are logged.

UTAdvanced Digital Indicating Controllers/Program Controllers/ Digital Indicator with Alarms

Write Access to Modbus Registers

Writing to Modbus registers over communication lines can be enabled or disabled. Disabling the feature will prevent outsiders with malicious intent from changing the controller settings. When the feature is disabled, settings must be changed manually onsite.

IP Access Limitation Function

Only Modbus access from a registered IP address is allowed. Access from an unregistered IP address is rejected. This feature prevents unauthorized access and enhances security.

YS1000 Series Single-loop Controllers

Write Access over Ethernet

Writing to Modbus registers over Ethernet can be enabled or disabled. Disabling the feature will prevent outsiders with malicious intent from changing the controller settings. When the feature is disabled, settings must be changed manually onsite.

7. Staff Security

One of the most important security threats is “people.” Human error can pose major security threats.

Education

The purpose of education is to ensure that staff members develop knowledge and skills about security and are able to carry out daily operations in accordance with security guidelines. Education should include the following objectives.

- Staff members deepen their understanding about security.
- Staff members recognize threats and influences on production control systems.
- Staff members can carry out appropriate security measures and improvements.
- Staff members understand the proper operation and management of production control systems. For example, staff members should learn how to check logs to determine whether a system has been attacked.

Education should be provided at the following occasions.

- At the time of employment
- When the staff members that access the applicable instruments change because of personnel changes or other reasons

Revision Information

Title : Recorders, Data Loggers, and Control Products Security Standard
Manual number : TI 04A02A01-00EN

June 2012/1st Edition
Newly published

October 2012/2nd Edition
Addition of the models (SMARTDAC+ GX/GP)

August 2015/3rd Edition
Addition of the models (SMARTDAC+ GM)

Written by Yokogawa Electric Corporation
Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Blank Page